POLSINELLI

150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

May 26, 2020

Michael J. Waters
(312) 463-6212
mwaters@polsinelli.com

Via Email (ATTORNEYGENERAL@DOJ.NH.GOV)

Attorney General Gordon J. MacDonald
Office of the Attorney General
Attn: Security Incident Notification
33 Capitol Street
Concord, NH 03301

Re: Notification of a Computer Security Incident Involving Personal Information Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Attorney General MacDonald:

We represent Compass Health, Inc., d/b/a Compass Health Network ("Compass") in connection with an incident that involved the personal information of one (1) New Hampshire resident, and provide this notice on behalf of Compass pursuant to N.H. Rev. Stat. § 359-C:20(I)(b). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Compass is notifying you of this incident, Compass does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY INCIDENT OR UNAUTHORIZED ACCESS

On or around March 20, 2020, PaperlessPay Corporation ("PaperlessPay") notified Compass of a security incident that it recently experienced. Compass contracts with PaperlessPay for the provision of online bi-weekly paystubs and W-2 tax forms. According, to PaperlessPay, on February 19, 2020, the Department of Homeland Security ("DHS") contacted PaperlessPay and notified it that someone was purporting to sell access to the PaperlessPay's client database on the dark web. PaperlessPay shut down its web server and SQL server to prevent unauthorized access. PaperlessPay worked with the Federal Bureau of Investigation ("FBI") and retained a cybersecurity firm to conduct a forensic investigation. The investigation revealed that someone accessed PaperlessPay's SQL server on February 18, 2020. Compass and PaperlessPay worked together to obtain additional information concerning the incident, including what, if any information the threat-actor may have acquired.

At this point, Compass is not aware of an unauthorized access or acquisition of its employees' personal information or that any of the information has been misused. However, PaperlessPay could not definitely rule out the possibility that someone accessed or acquired Compass' employees' personal information. Accordingly, Compass is notifying the potentially impacted employees and arranged for complementary identity theft protection services for the employees.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Compass determined that one (1) New Hampshire resident may have been impacted by this incident. Compass is notifying the impacted individual of the situation by letter today. Enclosed is a copy of the notice that is being sent to the impacted individual.

STEPS TAKEN RELATING TO THE INCIDENT

Upon becoming aware of the incident, Compass promptly investigated the incident to determine what, if any, personal information a third party might have acquired during the incident. Compass is also providing complimentary identity theft protection services to the impacted individual through Experian.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Michael J. Waters

Enclosure

Compass Health Network
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

[redacted]

May 26, 2020

Dear [redacted]

Re: Notice of a Security Breach

This letter follows on my prior communication regarding a data incident involving a Compass Health vendor called PaperlessPay Corporation ("PaperlessPay"). This letter provides some additional information about the incident and steps you can take to protect yourself from the misuse of your information. We have also arranged for complimentary credit monitoring and have included with this letter instructions on how you can sign-up for these services.

What Happened? On or around March 20, 2020, PaperlessPay notified us of a security incident that it had recently experienced. PaperlessPay is the company that we work with for the provision of online bi-weekly paystubs and W-2 tax forms. According to PaperlessPay, on February 19, 2020, the Department of Homeland Security ("DHS") contacted PaperlessPay and notified it that someone was purporting to sell access to the PaperlessPay client database on the dark web. In response, PaperlessPay shut down its web server and SQL server to prevent unauthorized access. It then worked with the FBI and retained a cybersecurity firm to conduct a forensic investigation. That investigation revealed that someone accessed PaperlessPay's SQL server on February 18, 2020. We have since been working with PaperlessPay to obtain more information about the incident. We understand that there is no evidence that the incident resulted in the unauthorized acquisition of any of our employees' personal information, but PaperlessPay also could not definitively rule out the possibility that someone viewed or acquired our employees' information, so we are providing notice to potentially impacted employees.

What Information Was Involved? The PaperlessPay server holds pay stubs and tax forms that contain information, including your name, address, pay and withholdings, part of the bank account number (first 5 digits are masked) if you have multiple accounts, and Social Security number.

What We Are Doing? We have arranged for a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B for all potentially impacted employees. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Experian IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on Experian IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do? While we have no evidence that anyone's personal information has been acquired or misused, you can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. I understand that you may have questions that this letter does not answer. If you have questions, please call 1-888-399-9989 from 8:00 a.m. to 5:00 p.m. CT, Monday-Friday.

Sincerely,

[redacted]

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC – Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting http://www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: If you are a resident of Maryland, you have the right to contact the Maryland Attorney General's office concerning the data security incident mentioned in this letter. Contact information for the Maryland Attorney General's Office is as follows: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, (410)-528-8662, consumer@oag.state.md.us.

North Carolina Residents: If you are a resident of North Carolina, you have the right to contact the North Carolina Attorney General concerning the Incident mentioned in this letter. Contact information for the North Carolina Attorney General's Office is as follows: North Carolina Attorney General's Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, (919)-716-6000.

Rhode Island Residents: We believe that this incident affected one Rhode Island resident. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.